TRICARE

TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Security Management Process

HIPAA Security • November 2003

Standard Requirement

Covered entities must implement a security management process as a part of their administrative safeguards. The HIPAA Security Rule defines that process as the implementation of "policies and procedures to prevent, detect, contain and correct security violations." The security management process and its related implementation specifications form the foundation of a covered entity's entire security program. This standard mandates a "life cycle approach" to security; that is to say, an organization must assess its security posture and work to reduce its risks on a continual basis as the security environment and needs of the organization change.

Required elements of the process are further defined through the four implementation specifications:

- risk analysis
- risk management
- a sanction policy, and
- an information system activity review.

Implementation Specifications

The first of the four implementation specifications, risk analysis, includes "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (EPHI) held by the covered entity." A risk analysis or risk assessment includes a threat assessment, vulnerability pairing, and residual risk determination. The risk analysis should include organizational and technical assessments that address all areas of security. A thorough and accurate risk analysis must consider "all relevant losses" that would be expected if security measures were not in place, including losses caused by unauthorized uses and disclosures as well as losses of data integrity or accuracy.

Building on risk analysis, the second implementation specification, risk management, requires implementation of security measures sufficient to reduce those risks and vulnerabilities "to a reasonable and appropriate level." The risk management process requires a covered entity to develop plans and take actions in response to the risk analysis as well as sponsor subsequent reassessments to determine the effectiveness of implemented safeguards.

Sanction policies must be in place to apply appropriate penalties and punishments against workforce members who fail to comply with the organization's security policies and procedures. Covered entities may use their standard disciplinary process to determine the specific sanction according to the severity and circumstances of the violation. The type

Security Management Process

and severity of sanctions imposed, and the categories of "violation," are left entirely to the determination of the covered entity.

The fourth implementation specification, information systems activity review includes implementation of "procedures to regularly review records of information systems activity, such as audit logs, access reports, and security incident tracking reports." It does no good to produce records of system use such as audit and system logs if no one ever examines them for potential breaches of security policy. HIPAA does not distinguish between automated or manual logs and reports in this requirement. Both must be reviewed. Again, HIPAA relies on a covered entity's risk analysis and risk management process to determine the frequency of these reviews.

See also:
45 CFR 164.308(a)(1)

Federal and DoD regulations that support this standard
OMB A-130 App. III
DoDI 5200.40
DoD 8510.1-M
DoDD 8500.1
DoDI 8500.2